INFORMACIJSKI POOBLAŠČENEC
Zaloška 59, 1000 Ljubljana, Slovenija
Telefon: 01 230 97 30
Faks: 01 230 97 78
E-pošta: gp.ip@ip-rs.si
www.ip-rs.si
REPUBLIKA SLOVENIJA

Zadeva: 007-25/2016/2
Datum: 10.5.2016

Dr. Ciril Keršmanc
Republika Slovenija
Ministrstvo za pravosodje
gp.mp@gov.si

ZADEVA: mnenje Informacijskega pooblaščenca k predlogu ZKP-N (EVA 2014-2030-0026, strokovno usklajevanje)
ZVEZA: Vaš dopis št. IPP 007-155/2016, z dne 6. 4. 2016

Spoštovani,

Informacijski pooblaščenec (v nadaljevanju IP) je prejel vaše zaprosilo za posredovanje pripomb k Predlogu sprememb Zakona o kazenskem postopku (ZKP-N) – EVA: 2014-2030-0026 (v nadaljevanju: predlog zakona). V nadaljevanju vam na podlagi 48. člena Zakona o varstvu osebnih podatkov (Ur. l. RS, št. 86/04, 113/05, 51/07 in 67/07, v nadaljevanju ZVOP-1) posredujemo pripombe IP k posameznim členom prejetega predloga ZKP-N.

K 3. členu predloga ZKP-N (sprememba 25. člena, pristojnost po stopnjah)

Prvi odstavek 3. člena predloga v 1. alinejo 1. odst. 25. člena ZKP vnaša izrecno pojasnilo, da je za obravnavo kaznivih dejanj zoper čast in dobro ime, storjenih na spletnih straneh, na sredstvih javnega obveščanja, ter preko sredstev javne priobčitve, namenjenih širšemu krogu ljudi, na prvi stopnji pristojno okrožno sodišče, vse iz razloga, da gre za kvalificirano obliko teh dejanj. Kar zadeva izvršitve na spletnih straneh, naj bi imela (kot navajate s sklicevanjem na komentar KZ-1, 2012) ta za oškodovanca »*najmanj enako hude posledice, kot velja za druge, izrecno navedene medije*«, še zlasti zaradi »*najširšega, svetovnega dosega spletnih strani in izjemne možnosti njihovega pregledovanja*«.

Zadevna materija sicer primarno spada v KZ-1, bi pa IP želel opozoriti na okoliščino, da vsakršne objave na spletni strani bržkone ni mogoče enačiti z objavo v »sredstvih javnega obveščanja« (oz. medijih). Sodna praksa višjega sodišča v Ljubljani[1] npr. določa, da t.i. »blog storitve« (v danem primeru Google Blogger) vsekakor sodijo med sredstva javnega obveščanja, in navedeno s stališča IP ni sporno. Po oceni IP pa je **težje trditi, da tudi npr. vse objave v zaprtih Facebook skupinah, zaprtih forumih, komentarjih pod novicami ali v okviru YouTube posnetkov, ali na prav vsaki spletni strani, ki jo je kdo kdaj postavil, dosegajo prag »izpostavljenosti« in »javne dosegljivosti«, ki jo imajo objave v sredstvih javnega obveščanja (oz. medijev),** kar naj bi posledično utemeljevalo večjo težo storjenega dejanja. Številne spletne strani so namreč vidne zelo malo očem, če sploh katerim, in jih tudi preko spletnih iskalnikov praviloma ni mogoče najti, ker njihova domena ni zadosti izpostavljena. Tudi na bolj izpostavljenih straneh obstajajo številni uporabniški vnosi, ki niso deležni nobenih ogledov (npr. številni YouTube posnetki). Posledično bi utegnilo biti pretirano, da se vsakršno žaljivo idr. objavo »na spletnih straneh« šteje za kvalificirano obliko pripadajočega kaznivega dejanja.

[1] VSL sodba II Kp 13079/2012, http://www.sodisce.si/vislj/odlocitve/2012032113073755/

Prav tako je termin »spletne strani« terminološko (kot terminus technicus) v marsičem nepopoln. Preko interneta, kot splošno dostopnega javnega omrežja, so namreč poleg svetovnega spleta (angl. World wide web, storitev gostovanja spletnih strani) dosegljive še številne druge storitve, med njimi npr. razne oblike klepetalnic in hipnega klepeta, VoIP storitve glasovnega pogovora, številne mobilne aplikacije, računalniške igre idr. Nekatere od teh storitev so tako ali drugače namenjene širši publiki. Izjave in medsebojni klepeti, izrečeni tam, so lahko prav tako širše vidni, kot tisti preko bloga ali drugih spletnih strani, namenjenih javnemu obveščanju. Posledično utegne zakonodajalec s pretirano podrobnim naštevanjem oblik »objave« izvotliti nujno potrebno splošnost (in tehnično nevtralnost), ki jo je KZ-1 pred novelo KZ-1B (ko je za »nove medije« uporabljal zgolj izraz »*z drugimi sredstvi javnega obveščanja*«) pravzaprav že imel. Podoben terminološki problem nastopi pri dodajanju izrazov »*gramofonske plošče, zgoščenke, filma, DVD-ja ali drugih videosredstev, zvočnih ali podobnih sredstev, namenjenih širšemu krogu ljudi*« med kvalifikatorne okoliščine za pristojnost okrožnih sodišč. Vsa izrecno našteta sredstva se danes že umikajo iz rabe, v prid digitalnega izdajanja vsebin - bodisi v obliki storitev videa na zahtevo (npr. Youtube, Netflix), ali preko različnih oblik naročnin (npr. Pandora ali drugi spletni radiji). Prihodnji razvoj bo gotovo prinesel še nove oblike.

Zatorej bi veljalo, tako v KZ-1, kot v ZKP, razmisliti o ohranitvi obstoječe dikcije, saj, kot že ugotavljajo sodišča (glej odkazano sodbo VSL), to povsem zadostuje za zajem tudi tistih spletnih in drugih internetnih storitev, ki so po naravi izpostavljenosti širšemu občinstvu resnično primerljiva s »*sredstvi javnega obveščanja*«.

Dalje predlagamo, da se razmisli, da se med pristojnosti pri okrožnem sodišču, ki je za to pristojno, doda tudi procesno dejanje obravnave pritožb tretjih oseb zoper odločitve pravosodnih organov (policije, tožilstva, sodišča) za posredovanje podatkov, izročitev predmetov, in druga podobna oblastna dejanja (t.i. motion to quash iz ameriških zveznih pravil o kazenskem postopku). Navedeno opcijo sicer podrobneje pojasnjujemo v komentarjih k členom o pridobivanju podatkov o prometu, oz. zasegu predmetov, spodaj.

K 10. členu predloga ZKP-N (nov 65.a člen, pravice oškodovanca)

65.a člen v našo zakonodajo prenaša obveznosti, ki izhajajo iz Direktive 2012/29/EU Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o določitvi minimalnih standardov na področju pravic, podpore in zaščite žrtev kaznivih dejanj ter o nadomestitvi Okvirnega sklepa Sveta 2001/220/PNZ (v nadaljevanju Direktiva 2012/29/EU). Direktiva 2012/29/EU, med drugim v 6. členu določa nabor informacij o poteku zadeve, ki naj jih država da na voljo žrtvi kaznivega dejanja, če ta zanje zaprosi.

Glede teh informacij 3. odst. novega 65.a člena določa pravico oškodovanca do prejemanja »informacij o stanju predkazenskega oziroma kazenskega postopka ter pravnomočnih obsodb« (§ 6(2) Direktive 2012/29/EU). Pravica se bo izvajala »preko [namenske] spletne strani«, v primeru večjega številka oškodovancev pa tudi preko spletnih strani policije, državnega tožilstva ali sodišča. Obveščanje bodo izvajali policija, državno tožilstvo oz. sodišča.

V danem primeru gre za posredovanje osebnih podatkov (o osumljencu in drugih osebah), zato IP predlaga, **da se obseg posredovanih informacij natančneje določi v zakonu, način njihovega posredovanja in druge tehnične podrobnosti, pa vsaj za najbolj pogoste primere, podrobneje opredeli v pravilniku MP** (ali navodilih, ki jih pripravijo zavezanci za obveščanje oškodovanca v sodelovanju z MP). Obseg posredovanih informacij naj se opredeli na način, da bo jasno omejen na potrebno za dosego cilja (da je žrtev »*seznanjena s stanjem kazenskega postopka*«). Kot navajate, policija prijaviteljem že omogoča

vpogled v stanje policijske preiskave preko spletne aplikacije[2] (če vnesejo svoje ime, EMŠO ter datum prijave), pridobijo pa lahko podatek o tem, ali je zadeva že zavedena v njihov sistem, ali preiskava še poteka, in če več ne, ali je bila v zvezi z njo podana ovadba oz. poročilo na državno tožilstvo. IP predlaga, da se podoben nabor določi tudi za kazenski del postopka. Obveznost priprave teh predpisov naj se določi v novem odstavku tega člena.

Smiselno bi bilo, da bi bil na ta navodila oškodovanec napoten v potrdilu, ki ga bo prejel po določbah novega 147.a člena.

Na tem mestu opozarjamo še na verjetno napako v slovenskem prevodu tč. (b) 1. odstavka 6. člena Direktive 2012/29/EU. Slovenski prevod[3] daje žrtvi pravico biti obveščena o »podrobnostih« o »stroških« zoper storilca, medtem ko angleški izvirnik uporablja besedo »charges«, kar na danem mestu pomeni kaznivo dejanje, katerega je storilec obdolžen oz. obtožen.

K 15. členu predloga ZKP-N (sprememba 84. člena, zavarovanje posnetka preiskovalnega dejanja)

IP predlaga, da se izraz »*kontrolna vrednost*« dopolni tako, da se bo glasil »*kontrolno vrednost in način njenega izračuna*«. Za naknadno preverbo kontrolne vrednosti je namreč treba razpolagati tudi s podatkom o tem, kateri matematični algoritem oz. kateri program je bil uporabljen za njen izračun. Tako je svoja interna navodila za zavarovanje digitalnih dokazov nedavno, na priporočilo forenzične stroke, posodobil tudi IP.

Isto spremembo velja seveda izvesti tudi v 5. odst. 223.a člena.

Novo predlagana sprememba 120. in 121. člena ZKP (vročanje pisanj s pritrditvijo na sodno desko)

Kot je IP že večkrat predlagal v svojih mnenjih (glej npr. mnenje IP št. 0712-1/2016/834, z dne 12. 4. 2016[4]), pri tovrstnem načinu vročanja z vidika načela sorazmernosti ni primerno, da se na sodni deski pisanje objavi v obliki, ki razkriva tudi osebne podatke tretjih oseb (oškodovancev, prič idr.). IP predlaga, da se 3. in 4. odst. 120. člena oz. 2. odst. 121. člena spremenita tako, da bi določala, da se na sodni deski objavi zgolj obvestilo o vročitvi, morebitni pravni pouk fikcije vročitve ter kraj, kjer posameznik lahko dvigne posamezen dokument (po vzoru ureditve v Zakonu o splošnem upravnem postopku).

K 24. členu predloga ZKP-N (dopolnitev 146. člena, ovadba)

Nov drugi odstavek ovaditeljem, ki so »*subjekti zasebnega prava*« dovoljuje, da ne glede na določbe drugih zakonov ovadbi priložijo tudi »*podatke, pridobljene pri ali v zvezi z njihovo dejavnostjo*«, četudi je z zakonom ali sklepom pristojnega organa določeno, da jih morajo varovati kot zaupne oziroma jih ne smejo razkriti drugim. Navedena določba torej celovito izključuje protipravnost takšnega posredovanja oz. ovaditeljevo odgovornost za sicer nezakonito razkritje podatkov.

Iz obrazložitve izhaja, da se za subjekte zasebnega prava štejejo zgolj pravne osebe, ne pa torej tudi fizične osebe (niti s.p.-ji, ki so še vedno fizične osebe, čeravno kot poslovni subjekti delujejo na trgu) in tudi ne njihovi zaposleni/uslužbenci oz. drugi posamezniki.

---

[2] http://www.policija.si/index.php/component/content/article/35-sporocila-za-javnost/77453-od-danes-deluje-nova-spletna-aplikacija-za-obveanje-okodovancev-kaznivih-dejanj
[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:315:0057:0073:SL:PDF
[4] https://www.ip-rs.si/vop/objava-sodnih-pisanj-na-oglasni-deski-in-spletu-2731/

Zdi se, da je krog tako privilegiranih (vnaprej splošno ekskulpiranih) ovaditeljev določen na dani način zato, ker se cilja zlasti na banke in hranilnice, da bi se za potrebe preiskave kaznivih dejanj v tem sektorju lažje odločale za sodelovanje z organi pregona, kar zadeva posredovanje dokazov, ki so sicer bančna tajnost. Če ima predlagatelj tak namen, IP predlaga, da se takšna določba raje zapiše v področne zakone (npr. ZBan-2, ali morda ZTP oz. ZGD-1).

Tako kot je določba sedaj zapisana, namreč po eni strani brez prave obrazložitve izloča fizične osebe in še zlasti zaposlene, ki bi načeloma imeli interes podati ovadbo, ne da bi nase prevzeli tveganje sledečega ločenega kazenskega postopka. Po drugi strani pa IP opozarja, da je določba pretirano široka in da nevarno posega v druge zakone, tako da določa svojevrstno univerzalno pravico posredovanja osebnih in vsakršnih drugih podatkov. Na njeni podlagi bi, denimo, lahko ponudniki javno dostopnih elektronskih komunikacij (operaterji) ali drugih storitev policiji posredovali prometne ali vsebinske podatke o komunikaciji njihovih uporabnikov ali celotne uporabniške baze[5]. Pri tem niso zamejeni s tem, da morajo biti dokazi po obsegu in vsebini dejansko primerni za dokazovanje ovadenega kaznivega dejanja (torej, sorazmerni), ampak lahko preprosto policiji posredujejo vse podatke, ki jih imajo o določeni zadevi. To bi, vsaj s stališča ZVOP-1, nesorazmerno posegalo v ureditev posredovanja osebnih podatkov.

IP zatorej predlaga, da se navedena določba bodisi precizira glede na zasledovane namene bodisi črta in prenese v druge (področne) predpise.

K 27. členu in 28. členu predloga ZKP-N (sprememba 148. in 148.a člena, formalno zaslišanje osumljenca brez navzočnosti zagovornika, nadzorstvena pritožba)

Spremenjeni 148. člen uvaja več novosti, in sicer:

1. širi možnosti vabljenja oseb na policijsko postajo (3. odst.);
2. predvideva možnost, da se osumljenca formalno zasliši brez prisotnosti zagovornika, če se osumljenec pravici do njegove navzočnosti odpove (dopolnjen 4. odst. in prenovljeni 148.a člen);
3. postopanje policije v primeru, da osumljenec uveljavi pravico do zagovornika (5. odst.), oz. da se ji molče odreče (da se začne sam izjavljati, 6. odst.);
4. podrobnejšo ureditev (nadzorstvene) pritožbe nad delom policije (7. odst.);
5. podrobnejšo ureditev komunikacije in koordinacije policije in državnega tožilca že pred zaključkom policijske preiskave in podajo kazenske ovadbe (9. in 10. odst.).

Čeravno zadevna dejanja policije oz. tožilca brez dvoma predstavljajo obdelavo osebnih podatkov v smislu ZVOP-1, gre po mnenju IP za materijo izrecno kazenskoprocesne narave, zatorej svoje mnenje k temu členu daje zgolj kot svoj prispevek, oz. priporočilo k medresorski razpravi. Dokončna odločitev o spremembah koncepta domačega kazenskega postopka namreč leži na predlagatelju, oz. zakonodajalcu.

Zadevši nove metode vabljenja (ustno, telefonsko, po elektronski poti), vsakič s primernim pravnim poukom, IP nima dodatnih pripomb.

Spremenjeni 148.a člen pomembno širi možnost formalnega zaslišanja osumljenca s strani policije oz. tožilstva, torej tako, da imata nastali zapisnik o zaslišanju (oz. zvočni in video posnetek) dokazno vrednost v kasnejšem sodnem postopku, in ne zgolj naravo uradnega zaznamka, ki sicer lahko ostane v spisu, ne more pa sodišče nanj opreti svoje odločbe. Konkretno dopušča, da se osumljenca tako zasliši tudi brez prisotnosti

[5] V ZDA je bil v to smer predlagan zakon CISPA (Cyber Intelligence Sharing and Protection Act, https://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act), ki bi podjetja iz IT branže imuniziral v primeru širokega sodelovanja z domačimi pravosodnimi organi. Predlog je bil vse od vložitve l. 2011 deležen širokega nasprotovanja s strani internetne industrije, in je bil sprejet šele lani decembra, »skrit« kot priloga zakona o zveznem proračunu.

zagovornika, če se tej pravici odreče, in če se zaslišanje zvočno oz. slikovno posname. IP glede te ureditve **opozarja, da utegne priti do posega v osumljenčev privilegij proti samoobtožbi, v kolikor se istočasno ne popravi 70. člena ZKP na način, da bo osumljencu, ki si zagovornika ne more privoščiti sam, na voljo zagovornik po uradni dolžnosti.** Policijsko (oz. policijsko-tožilsko zaslišanje), čeravno izvedeno na podlagi vabila (ne privedbe, kjer bo obramba še naprej obvezna) vedno predstavlja dejanje osredotočene policijske preiskave, kar pa je že tisti trenutek, ko zapadejo vse osumljenčeve pravice, vključno s pravico do zagovornika, ki mora biti osumljencu, če si ga sam ne more privoščiti, zagotovljena po uradni dolžnosti, oz. bi mu bila, če bi zaslišanje opravil preiskovalni sodnik, morala biti zagotovljena (4. odst. 70. člena ZKP v zvezi s 1. odst. istega člena). Navedeno utemeljujemo v nadaljevanju.

Možnost formalnega zaslišanja osumljenca s strani policije je bila v ZKP prvič dodana z novelo ZKP-E (2003)[6], v odziv na odločbo Ustavnega sodišča št. U-I-92/96, z dne 28. 3. 2002, v kateri je sodišče potegnilo ločnico med predkazenskim postopkom in kasnejšima sodnima fazama postopka (kot sta veljali v takrat veljavnem ZKP).[7] Posledično je zakonodajalcu naložilo (evidenčni stavek sodbe), da dosledneje zagotovi, da »*se razpravljajoči sodnik [ne] seznani z obvestili, ki jih pridobi policija v predkazenskem postopku (ki morajo biti sicer izločena iz spisa in se nanje sodba ne sme opirati)*«, oz. v primeru, da je do tega prišlo, poskrbi za izločitev takšnega sodnika. Zakonodajalec je s sprejemom ZKP-E tem navodilom o izločanju gradiva iz spisa sledil, vendar pa se je v noveli istočasno odločil (kar je sodišče v svoji odločbi tudi dopuščalo) **postopoma začeti spreminjati koncept kazenskega postopka**, tako da bi v njega (glej primerjalnopravni pregled v predlogu, povezava v opombi) vnesel več akuzatornih elementov. Specifično, uvedel je možnost da policija osumljenca že v predkazenskem postopku zasliši na način, ki bo imel dokazno vrednost: *»S predlaganim postopnim razširjanjem pooblastil policije v predkazenskem postopku se njenim dejanjem pri izbiranju obvestil odvzame dosedanja narava "prepovedanih dokazov", katerih navzočnost v spisu lahko privede celo do izločitve sodnika.*[8] ***Z navzočnostjo zagovornika opravljeno zaslišanje pa pridobi naravo pravega dokaza, na katerega se lahko opira sodna odločba**. Dosedanjo naravo prepovedane vsebine, ki mora biti izločena iz spisa, bodo tako imeli le zaznamki o razgovorih policije z osumljencem, opravljeni preden je bil predkazenski postopek nanj utemeljeno usmerjen ("osredotočeno preiskovanje")…«* torej brez predhodnega pravnega pouka po spremenjenem četrtem odstavku 148. člena zakona.

ZKP-E je torej policiji, kot organu odkrivanja kaznivih dejanj in njenih storilcev, dovolil zbirati dokaze, pri tem pa je, zavoljo zagotovitve osumljenčeve pravice, da ni dolžan izpovedati zoper sebe ali svoje bližnje, ali priznati krivdo (4. al. 29. člena Ustave RS, pravna jamstva v kazenskem postopku) zahteval, da mora biti pri zaslišanju prisoten zagovornik, zato da zagotovi »enakost orožij« osumljenca – ki je v danem trenutku praviloma že pridržan – in policije.

ZKP-N, kot navajate v uvodni obrazložitvi, nadaljuje po začrtani poti postopnega uvajanja novega modela kazenskega postopka in s tem povezane možnosti opravljanja formalnih preiskovalnih dejanj že v predkazenskem postopku, s strani policije oz. tožilstva. V danem členu se predlaga, da se da osumljencu možnost, da se **pravici do prisotnosti zagovornika odreče**, razen v primerih, **ko je obramba v tej fazi**

[6] Besedilo novele: http://www.uradni-list.si/1/objava.jsp?sop=2003-01-2770, predlog novele: http://www.dz-rs.si/wps/portal/Home/deloDZ/zakonodaja/izbranZakonAkt?uid=C12565D400354E68C1256CE6003144DD&db=kon_zak&mandat=III&tip=doc

[7] Sodišče je takrat v pripadajočem tiskovnem sporočilu zapisalo, da »namena zbiranja obvestil v fazi predkazenskega postopka ni mogoče enačiti z namenom zbiranja dokazov in podatkov v fazi preiskave, še manj pa z namenom izvajanja dokazov v fazi sojenja. V fazi sojenja lahko sodnik, ki odloča na podlagi opravljene ustne glavne obravnave, v skladu z načelom neposrednosti opre sodbo samo na dejstva in dokaze, ki so bili pretreseni na glavni obravnavi. Iz tega izhaja, da se razpravljajoči sodnik ne sme seznaniti z obvestili, danimi v prvi fazi postopka, zato jih mora preiskovalni sodnik po koncu preiskave izločiti iz spisa«.

[8] Po novem tako tudi brez navzočnosti zagovornika opravljeni razgovori z osumljencem, ob uvedbi obveznosti popolnega pravnega pouka ("Miranda rule") o pravicah v postopku - postanejo dovoljeno spisovno gradivo, ki ga ni potrebno izločiti, čeprav se sodba nanj ne more opirati.

postopka obvezna[9], pri čemer naj bi se nastali »primanjkljaj« pri zagotavljanju njegovega privilegija pred samoobtožbo zagotovilo tako, da bo zaslišanje treba v celoti zvočno oz. slikovno posneti, ter da se podrobneje predpiše potek zaslišanja (prisotnost oz. obvezna prisotnost tožilca, prisotnost pouka in odreka pravici do odvetnika na posnetku, prepoved kapcioznih oz. sugestivnih vprašanj ali drugačnih preslepitev pri zasliševanju).

IP opaža več težav, do katerih bi lahko pripeljala takšna ureditev:

1. odrek pravici do zagovornika dejansko ni odrek, če osumljenec takšne pravice ni sposoben dejansko izvrševati, ker si zagovornika ne more privoščiti; posledično bi veljalo razmisliti o ureditvi, po kateri bi se za policijsko zaslišanje po 148.a členu s popravkom 4. odst. 70. člena določilo pravico do pridobitve zagovornika po uradni dolžnosti, kot bi sicer osumljencu pripadala pri prvem zaslišanju pred preiskovalnim sodnikom (po 157. členu ZKP); obveznost snemanja tega ne more nadomestiti;
2. ureditev iz 5. odst. 148. člena še vedno dopušča manevrski prostor, da policija po tem, ko osumljenec zahteva odvetnika, pa odvetnika še ni, oz. ne pride pravočasno, sploh ne pride, oz. že odide, sama ponovno začne zaslišanje, in s tem poseže v njegovo že izrečeno pravico, da bo zaslišan samo v prisotnosti zagovornika. Odločitev osumljenca, da se brani z molkom, posledično ne bo dosledno spoštovana, dokazovanje tega pa bo težko; aktivnosti policije v smer priprave osumljenca, da poda izjavo (in inkriminira sebe oz. druge), namreč ne bodo zabeležene na posnetku, saj se bo snemanje začelo šele naknadno, po tem, ko je osumljenec prepeljan v namenske prostore (kjer bodo potem posneti samo pouk, odrek, in izjava). Zato bi veljalo razmisliti o spremembi 5. odst. 148. člena in izrecni določitvi, da policija po tem, ko osumljenec izjavi, da si bo vzel zagovornika, ne sme več sama začeti zasliševanja ali drugega procesnega oz. preiskovalnega dejanja (razen če bi bilo nujno odlašati); ne zgolj, da je treba s tem počakati;
3. po drugi strani ni prepričljivega razloga, zakaj se pravici biti zaslišan ob prisotnosti odvetnika ne bi smela odreči oseba, ki je pridržana, priprta, ali osumljena težjega kaznivega dejanja;[10] Prav tako ni pravega razloga, da se ji ne bi oseba smela odpovedati tudi, kadar je osumljena težjih kaznivih dejanj; to še toliko bolj, ker bo za pravilnost zaslišanja tam skrbel tudi državni tožilec, ki bo (razen izjemoma) moral biti prisoten in bo moral sam izvajati zaslišanje.

Upoštevajoč navedeno se zdi pravilneje, da se vse osumljence – tiste, ki na zaslišanje pridejo prostovoljno in na podlagi vabila, kot tudi tiste, ki jim policija odvzame prostost in jih pridrži v svojih prostorih – obravnava enako.[11] S tališča pripada privilegija je vseeno, kako je policija prišla do te točke.[12] Četudi je prišel prostovoljno, in ima (vsaj načeloma) po prejemu pouka pravico oditi, ker niso podani razlogi za pridržanje, je treba glede na vse okoliščine, v katerih se izvaja zaslišanje (v namenskih policijskih prostorih, pod kamero, kjer je osumljenec praviloma sam – dokler seveda nima zagovornika – in v položaju proti enemu ali več policistov in tožilcev), šteti, da gre za *kustodialno* zaslišanje.

---

[9] Primeri, ko se je osumljenec nezmožen se je sam braniti, v policijskem pridržanju, ali obtožen hudega kaznivega dejanja – smiselno po 70. členu ZKP.

[10] Pravica do obvezne obrambe je pravica, ki se ji osumljenec lahko odpove; morda je v kasnejši sodni fazi postopka (po privedbi k preiskovalnemu sodniku oz. drugačnemu začetku sodne faze postopka) potrebno, da to odpoved potrdi še sodnik, vendar pri osebah, ki so se sposobne same braniti, načeloma mora obstajati. Ključno je, da pravica obstaja, torej da jo osumljenec lahko izkoristi, če jo želi. Če se ji namreč lahko odreče med prvim policijskim zaslišanjem, in s tem z veliko verjetnostjo postavi v položaj, da bo priznal očitano kaznivo dejanje oz. se drugače inkriminiral ter s tem v veliki meri že »zapečatil« usodo v nadaljnjem postopku, ne more biti razloga, da se tej pravici ne bi smel odpovedati tudi v kasnejših fazah postopka (ko je že pridržan ali priprt).

[11] Privilegij zoper samoobtožbo, kot izhaja iz 4. al. 29. člena Ustave, v vsakem primeru zapade, ko se policijska preiskava osredotoči na določeno osebo. To je takrat, ko policija preneha poizvedovati o tem, ali je bilo dejanje storjeno, ter kdo bi lahko bili osumljenci, in ima že razloge za sum, da je prav ta določena oseba storila kaznivo dejanje. V tistem trenutku je treba temu osumljencu podati dolžni pravni pouk (4. odst. 148. člen), pripadejo pa mu pravice iz tega pouka oz. druge pravice po zakonu (npr. po 5. členu ZKP).

[12] Lahko je storilca zaznala in flagrante, lahko je bil vabljen kot tak in je na policijsko postajo prišel prostovoljno, ali je bil tja priveden, lahko je bil pridržan, lahko je bil tudi vabljen kot priča ali tretja oseba, pa se je med razgovorom razkrilo, da zoper njega obstojijo razlogi za sum.

Zatorej bi veljalo razmisliti o rešitvi, da se položaj za vse osumljence poenoti, tako da se iz 3. odst. 148.a člena črta navedek, da osumljenec ne sme biti zaslišan tudi brez prisotnosti zagovornika, »*če je pridržan, (priprt), ali osumljen kaznivega dejanja, za katerega je v zakonu predpisana kazen zapora osmih ali več let*«. Pripadajoče bi veljalo dopolniti tudi določbe o obvezni obrambi iz 1. odst. 70. člena, tako, da mora osumljenec že na prvem zaslišanju, policijskem ali ne, imeti pravico do zagovornika, po potrebi imenovanega po uradni dolžnosti, medtem ko naj obvezna obramba (ki se ji ne more odreči) ostane v predkazenskem postopku v primerih, ko ni sposoben, da se sam brani, v sodni fazi postopka pa še vedno. Takšna sprememba bi upoštevajoč navedeno pomenila uresničitev cilja novele, to je opolnomočenje policije in tožilstva, da opravijo ključna preiskovalna dejanja že v predkazenskem postopku.

Poleg tega bi bilo smiselno razmisliti tudi o spremembi 5. odst. 148. člena s ciljem pojasnitve, da v primeru, da osumljenec izjavi, da želi zagovornika, policija do njegovega prihoda ustavi vsa procesna dejanja oz. preiskovalna dejanja, ki tako ali drugače zahtevajo osumljenčevo aktivnost (dajanje izjav, pojasnil, pomoč pri iskanju predmetov kaznivega dejanja idr.), razen če bi jih bilo nevarno odlašati, odložiti ali prekiniti. Če je namreč osumljenec izjavil, da brez prisotnosti zagovornika ne želi sodelovati, je to njegova pravica iz privilegija zoper samoobtožbo, in policija sama ne sme več prožiti iniciativ za njegovo sodelovanje.

K 29. členu predloga ZKP-N (nova 148.b in 148.c člen, ex parte zaslišanje priče v predkazenskem postopku)

Novi 148.b člen predvideva možnost zaslišanja priče s strani državnega tožilca in policije, torej brez prisotnosti osumljenca. Njegova pravica do soočenja priče se potem zagotovi tako, da mu mora biti dana možnost naknadnega soočenja, sicer sodišče svoje odločbe ne bo smelo opreti na zapisnik o zaslišanju (razen če priča iz objektivnih razlogov takrat ne bo več dosegljiva sodišču).

IP bi upoštevajoč zgoraj navedeno zgolj informativno želel izpostaviti, da se po nam znanih podatkih zaradi zagotovitve načela kontradiktornosti predhodno zaslišanje prič (v ameriški praksi *deposition*) izvaja zgolj izjemoma, t.j. če je pričakovati, da priča tekom sojenja ne bo dosegljiva, ali če so podane kakšne druge okoliščine, tako da se v predkazenskem postopku od nje skoraj vedno zbirajo zgolj obvestila. Tudi če je tako, mora imeti obdolženec še vedno pravico, da je prisoten na takšnem zaslišanju, da jo lahko sooči. Naknadno soočanje namreč trpi določene omejitve, sicer značilne za posredne dokaze, kot so nevarnosti, da si priča naknadno premisli, ali da pozabi, ali da je bila prvotno neiskrena.

V vsakem primeru se tovrstna zaslišanja praviloma izvajajo na podlagi odredbe sodišča, kar pomeni, da dejstvo, ali bo zaslišanje lahko izvedeno oz. posneto, ne bo odvisno od volje priče, da sodeluje.

K 30. členu predloga ZKP-N (sprememba 4. odst. 149.a člena, prečiščen katalog kaznivih dejanj, v zvezi s katerimi je dovoljena raba ukrepa tajnega opazovanja oz. pridobivanja shranjenih podatkov o prometu)

S spremembo se prečiščuje in deloma dopolnjuje katalog tistih hujših kaznivih dejanj, glede katerih bo dopustno uporabljati prikrita preiskovalna ukrepa tajnega opazovanja in – s spremembo 149.b člena, tudi ukrep pridobivanja podatkov o prometu za nazaj (ki je bil do sedaj dopusten za vsa kazniva dejanja, ki se preganjajo po uradni dolžnosti). Spremenjen katalog je po eni strani nekoliko širši, po drugi pa ožji, zlasti z izključitvijo kaznivih dejanj, ker rabe omenjenih ukrepov po mnenju predlagatelja ni bilo mogoče utemeljiti z vidika sorazmernosti (npr. navadne tatvine, zatajitve, ali prikrivanja).

Do kataloga za rabo ukrepa po 149.a členu IP nima nadaljnjih pripomb, se pa ne strinja, da, kot navajate, »*ni videti utemeljenega razloga*«, da ga ne bi bilo mogoče uporabiti tudi za rabo ukrepa pridobivanja podatkov o

prometu za nazaj (torej shranjenih prometnih podatkov). IP predlaga, da se namesto tega **za ukrep po 149.b členu uporabi katalog po 2. odstavku 150. člena ZKP**, ki na splošno dopušča tista kazniva dejanja, kjer je zagrožena kazen vsaj 8 let, ne pa vsaj 5, kot pri katalogu za 149.a člen, ki se ga po potrebi dopolni z posameznimi kaznivimi dejanji, kjer potrebe prakse kažejo na sorazmernost rabe ukrepa.

IP potrebo po strožjem pristopu do ukrepa po 149.b členu najprej utemeljuje z več argumenti.

Prvič, Ustava RS primerjalnopravno zagotavlja eno najvišjih ravni varstva komunikacijske zasebnosti, višjo od večine drugih držav in od mednarodnih dokumentov[13], in tudi višjo od ravni varstva splošne zasebnosti (v katero sicer posega ukrep tajnega opazovanja), prostorske zasebnosti (v katero posega zlasti hišna preiskava), oz. informacijske zasebnosti (v katero posegajo številne določbe tako ZKP, kot ZNPPol, kot tudi drugih zakonov iz delovnega področja pravosodja). Zaradi pomena, ki ga imajo komunikacije na daljavo v moderni dobi, ter istočasno dejstva, da te komunikacije tipično potekajo preko posrednikov in da se torej država z njimi lahko **enostavno in hitro seznani**, **velja komunikacijsko zasebnost varovati strožje**[14].

Policiji osumljenca ni treba neposredno opazovati, da bi nadzorovala njegove komunikacije; posledično **dobi vsebinsko mnogo globlji in vsebinsko širši vpogled v njegovo zasebnost**[15]. Teža posega je zatorej po intenzivnosti višja, temu primerno bi morali biti kriteriji za poseg tudi bolj zahtevni. Zanimivo primerjavo tukaj nudi ločnica med tajnim opazovanjem, ki ga lahko odobri že državni tožilec (5. odst. 149.a člena) in tistim, ki ga že mora odobriti preiskovalni sodnik. Tožilec lahko odobri blažjo obliko posega, t.j. neprekinjeno ali ponavljajoče opazovanje in sledenje, osredotočeno zgolj na spremljanje položaja, gibanja ali aktivnosti osumljenca oz. izjemoma tretje osebe, vse na javnih krajih ali vsaj iz z javnega kraja vidnih krajih. Kolikor želi policija uporabiti tehnična sredstva za ugotavljanje položaja (npr. pritajeni GPS oddajnik na osumljenčevem vozilu), mikrofone, ali opazovati osumljenca v zasebnih prostorih, sicer z dovoljenjem imetnika, je za to že potrebna sodna odredba.

Na prvi pogled se torej zdi, da bi preiskovalni sodnik že na podlagi tega člena lahko odredil sledenje s pomočjo lokacijskih podatkov, ki jih o osumljenčevem mobilnem telefonu hrani tudi operater, vendar stroka opozarja, da ti dve situaciji nista analogni, kot je pojasnjeno v Komentarju Ustave Republike Slovenije: [*Postavlja se pomembno vprašanje, ali je mogoče omenjeni člen uporabiti za sledenje uporabnika komunikacijskega sredstva z nadzorom lokacijskih podatkov. Odgovor je brž kone negativen. Zgolj ob uporabi nedopustne preširoke pravne analogije pa bi jo bilo mogoče razširiti tudi na posege v lokacijske podatke, ki jih vodijo operaterji k. storitev na podlagi ZEKom-1. [..] Iz tega sledi, da je* ***sledenje gibanja uporabnikov v realnem času preko lokacijskih podatkov dopustno zgolj in samo ob strožjih pogojih iz 150. člena ZKP, medtem ko bi 149.a člen ZKP prišel v poštev zgolj v primeru, da bi bila v telefon nameščena od operaterja neodvisna GPS naprava***.][16]. Če tako velja že samo za lokacijske podatke, ki so zgolj (manjši) del prometnih podatkov, potem mora to veljati še toliko bolj za podatke o sami komunikaciji, iz katerih je nesporno mogoče izluščiti zelo natančne ugotovitve o zasebnem življenju osumljenca. Poseg v komunikacijsko zasebnost je hujši od posega v lokacijsko zasebnost oz. splošno zasebnost in mora biti zato dovoljen v zvezi z ožjim naborom kaznivih dejanj.

Drugič je mogoče nekatere namige poiskati v zadevni odločbi Ustavnega sodišča št. U-I-65/13, z dne 3. 7. 2014[17]. Z njo je sodišče razveljavilo določbe ZEKom-1, ki so operaterjem (torej ponudnikom splošnih, javno dosegljivih komunikacijskih storitev) nalagale obvezno hrambo podatkov o prometu o telefonskih in drugih

[13] Lovro Šturm (urednik), Komentar Ustave Republike Slovenije, Fakulteta za državne in evropske študije, Kranj, 2011, poglavje o komunikacijski zasebnosti, tč. 8.
[14] Tako Ustavno sodišče izrecno tudi v odločbi št. U-I-25/95 z dne 27. 11. 1997, http://odlocitve.us-rs.si/sl/odlocitev/US18710, glej prvi evidenčni stavek: "Ustava tisti del zasebnosti, ki se nanaša na svobodo komuniciranja, varuje dvakrat: v 35. členu, kjer postavi pravilo, da ima vsakdo pravico do zasebnosti in da je zasebnost nedotakljiva, in še posebej v 37. členu, s katerim zagotavlja tajnost pisem in drugih občil. Pogoje za omejitev te pravice vsebuje drugi odstavek 37. člena Ustave."
[15] Glej npr. nekatere tuje študije o sporočilnosti prometnih podatkov, http://www.zeit.de/datenschutz/malte-spitz-data-retention oz. http://news.stanford.edu/news/2014/march/nsa-phone-surveillance-031214.html , oz. v poljudni obliki, https://www.eff.org/deeplinks/2013/06/why-metadata-matters
[16] ibid, tč. 26 poglavja o komunikacijski zasebnosti
[17] http://odlocitve.us-rs.si/sl/odlocitev/US30439

(zlasti internetnih) komunikacijah za obdobje 14 oz. 8 mesecev. Pri tem je izhajalo iz ugotovitve, da so s to hrambo nastale obsežne zbirke, ki nesporno omogočajo »*izluščit[ev] zelo natančne ugotovitve o […] zasebnem življenju [uporabnikov storitev, to pa je pretežni del vseh domačih fizičnih in pravnih oseb]*«, v kombinaciji s premalo zamejenimi možnostmi za pridobivanje teh podatkov in nezmožnostjo posameznikov, da so obveščeni o tej uporabi, pri posameznikih *»ustvari[jo] (ne »bi lahko ustvarile«, op. IP) neoprijemljivi občutek stalnega nadzora, to pa lahko vpliva na izvrševanje drugih pravic, predvsem pravice do svobodnega izražanja in obveščanja (prvi odstavek 39. člena Ustave)«.*

Ukrep zbiranja, za potrebe kasnejše uporabe, je pri tej presoji sicer označilo kot sledeč zakonitemu cilju in kot primeren, vendar ne nujno potreben in zato neustaven, ker **neselektivno hrani** podatke o vseh komunikacijah, vključno s privilegiranimi (zaupna razmerja), in ker pridobivanja s **»skrbno odmero okoliščin« ni zamejil na tisto, kar je »nujno potrebno« za dosego namena – preprečevanja, preiskovanja in pregona hudih oblik kaznivih dejanj.**

Sodišče pri tem pojma »hudih« kaznivih dejanj neposredno ni definiralo, ampak je to nalogo prepustilo zakonodajalcu. Dalo pa je določene namige, npr. v 23. točki, kjer ugotavlja, da je boj proti takšnim hudim kaznivim dejanjem, kot so *»organiziran[i] krimina[l] in teroriz[em], obramba države in zagotavljanje nacionalne varnosti ter ustavne ureditve«,* temeljnega pomena za delovanje pravne države.[18] Dejstvo je torej, da sodišče na več mestih namiguje na katalog po 150. členu kot tisti, kjer je nujnost ukrepa hrambe oz. pridobivanja lahko izkazana. Bolj podroben namig pa daje pritrdilno ločeno mnenje takratnega ustavnega sodnika Boštjana M. Zupančiča k odločbi št. U-I-25/95 z dne 27. 11. 1997, v kateri je s sistematično razlago 2. odst. 37. člena zapisal: »*Ko je ustavodajalec v drugem odstavku 37. člena zapisal, da je poseg v nedotakljivost človekove zasebnosti dopusten samo, če je to nujno za varnost države, je s tem implicitno postavil merilo tudi za vprašanje nujnosti uvedbe in nadaljevanja kazenskega postopka. Povsem jasno je namreč, da grobi državni vpad v zasebnost posameznika* ***ne more biti dovoljen glede vsakega kazenskega postopka****, to je glede kateregakoli kaznivega dejanja. Tak poseg je lahko* ***dovoljen samo pri tistih kaznivih dejanjih, ki se po svoji družbeni nevarnosti približujejo ravni napada na varnost države kot celote«****.*

Tretjič, in končno, nuje uporabe ukrepa pridobivanja prometnih podatkov za nazaj za tista kazniva dejanja, ki bi bila zajeta s katalogom po 149.a členu ZKP, ne pa s katalogom po 150. členu ZKP, ne opravičuje statistika. IP je seznanjen s preliminarno statistično obdelavo cca. 14-mesečne uporabe ukrepa po 149.b členu ZKP, ki jo je pripravilo ministrstvo za notranje zadeve, in iz katere izhajajo sledeče ugotovitve:

- da se odredbe za uporabo ukrepa v številnih primerih (približno 25%, zlasti tatvine po 204. členu) uporabljajo za kazniva dejanja, ki po teži ne dosegajo niti tistih iz (tukaj dopolnjenega) 149.a člena, in kjer torej pridobivanje za nazaj v vsakem primeru ne bo mogoče;
- da bi praktično edina razlika nastopila glede ukinitve možnosti uporabe ukrepa za preiskavo kaznivega dejanja velike tatvine (razen če bi šlo za sum tatvine v okviru hudodelske združbe, se pravi organiziranega kriminala), torej verjetno pri ne bistveno več kot 10% odredb. Ostala kazniva dejanja, ki so v katalogu po 149.b členu, ne pa po 150. členu, in za katere so bile izdane odredbe, pa predstavljajo manj kot 2% izdanih odredb;
- da je mogoče sklepati, da bi večino preiskovanih dejanj, kjer bi policija izgubila možnost uporabe ukrepa za nazaj, lahko vseeno rešili z rabo ukrepa za naprej, oz. na druge načine, kar bi spet pomenilo, da pridobivanje podatkov za nazaj ni nujno.

Posledično IP predlaga, da se upošteva posebni ustavnopravni položaj podatkov o prometu, ter dostop do njih temu primerno zameji na preiskovanje in dokazovanje kaznivih dejanj iz istega kataloga, kot velja za izvedbo prisluhov.

[18] Podobno v 27. točki, kjer zakonodajalcu očita, da se v 149.b členu ZKP ni zamejil zgolj na določena (huda) kazniva dejanja , za katera bi ocenil, da »*zaradi njihove teže hramba podatkov oziroma dostop do njih upravičujeta poseg v zasebnost posameznika*«. Z opombo št. 33 pa kaže na primer, kjer je takšna razločitev bila izvedena, in to ravno z razliko med katalogoma po 149.a in 150. členu (kot že argumentirano spodaj).

K 31. in 32. členu predloga ZKP-N (spremenjeni 149.b člen, novi 149.c, 149.č in 149.d členi, nova ureditev pridobivanja podatkov o prometu)

Kot izhaja iz uvodne obrazložitve, se z novelo ZKP-N tudi »*bolj jasno in določno ter ustavnoskladno*« ureja vprašanje uporabe prikritega preiskovalnega ukrepa pridobivanja podatkov o prometu. Vzgiba za prenovo obstoječega 149.b člena ZKP sta, glede na obrazložitev člena, dva: prvič, uskladitev ukrepa z predlansko odločbo Ustavnega sodišča št. U-I-65/13, z dne 3. 7. 2014[19] o razveljavitvi obvezne hrambe podatkov o prometu pri operaterjih, ter drugič, razrešitev nekaterih praktičnih dilem, kot so možnost pridobivanja podatkov tudi od ponudnikov komunikacijskih storitev, ki niso operaterji , še zlasti od ponudnikov spletnih in mobilnih storitev, možnosti zasebnega tožilca v tej smeri, ter možnost pridobivanja naročniških podatkov brez sodne odredbe.

Nova ureditev tako razširja in razčlenjuje možnosti policije za pridobivanje podatkov o prometu o elektronskih komunikacijah. Izrecno dovoljuje pridobivanje podatkov o prometu tudi od ponudnikov komunikacijskih storitev, ki niso operaterji v smislu ZEKom-1 (kar je sicer po mnenju IP že bilo dopustno s smiselno rabo 143. člena ZKP, glej npr. mnenje št. 0712-1/2014/711, z dne 20. 2. 2014[20]). Obenem ločeno ureja (*»niansirani pristop«, »glede na različno intenzivnost in kvaliteto posega«, kot navajate v obrazložitvi*) pridobivanje podatkov za nazaj (se pravi - shranjenih, retencijskih podatkov), kar dopušča za huda kazniva dejanja, ter pridobivanje podatkov za naprej (t.i. *data freeze* oz. *data preservation* po Konvenciji Sveta Evrope o kibernetskem kriminalu), kar dopušča tudi za lažja kazniva dejanja. Prav tako posebej ureja zahtevke policije za naročniške oz. imeniške podatke (3. odst. obstoječega 149.b člena ZKP, zdaj 149.č ZKP), oz. tovrstne zahtevke zasebnega tožilca (149.d člen ZKP). Vsi členi tudi jasneje določajo, katerih podatkov se na njihovi podlagi ne sme pridobivati (»*ustrezne sistemske varovalke pred zlorabami*«), kar je po mnenju IP pozitivno, glede na številne v praksi ugotovljene težave pri njegovi uporabi (glej npr. Poročilo IP o uporabi pooblastil za posredovanje osebnih podatkov uporabnikov spletnih strani z vsebino, ki jo posredujejo prejemniki storitve, za leto 2015[21]).

Nova ureditev, kot se zdi, tudi znova določa, da se podatki o prometu posredujejo preiskovalnemu sodniku (ki jih potem posreduje policiji) in ne več neposredno organu, ki zanje izvorno zaprosi (policija oz. državni tožilec). Slednji režim je bil v ZKP uveden leta 2001 z novelo ZKP-K[22], glede na besedilo takratnega predloga (k 21. členu, str. 63) iz razlogov »*informatizacije in avtomatizacije*« postopkov posredovanja podatkov od operaterja do policije, kar naj bi bilo namenjeno »*povečanju učinkovitosti, preglednosti in varnosti podatkov*«.

Kot ugotavlja IP, iz predloga ZKP-N ni povsem jasno, ali gre za načrtno spremembo ali ne. Možnost posredovanja preiskovalnemu sodniku je namreč izrecno omenjena kot svojevrstno pravno sredstvo pri ukrepu po 149.č členu ZKP, prav tako se izrecno uvaja naknadna kontrola zakonitosti ukrepa s strani preiskovalnega sodnika v 153. členu ZKP. IP poudarja, da je takšna sprememba pomembna zlasti kot oblika vnaprejšnje kontrole zakonitosti ukrepa (t.j. preden pridobljeni podatki pridejo do policije), predvsem zaradi številnih v praksi zaznanih težav pri uporabi 149.b člena ZKP.

IP se do posameznih členov iz skupine 149.b – 149.d členov ZKP opredeljuje posebej.

[19] http://odlocitve.us-rs.si/sl/odlocitev/US30439
[20] https://www.ip-rs.si/vop/posredovanje-podatkov-o-ip-naslovu-bralca-2336/
[21] https://www.ip-rs.si/fileadmin/user_upload/Pdf/clanki/Porocilo_posredovanje_podatkov_o_uporabnikih_interneta_jan2016.pdf
[22] Besedilo novele, http://www.uradni-list.si/1/objava.jsp?sop=2011-01-3914, besedilo predloga http://www.dz-rs.si/wps/portal/Home/deloDZ/zakonodaja/izbranZakonAkt?uid=C12565D400354E68C12578A3005502D8&db=kon_zak&mandat=V&tip=doc

K spremenjenemu 149.b členu ZKP - pridobivanje podatkov za nazaj (torej shranjenih podatkov)

Kot že rečeno pri prejšnji točki, IP meni, da bi lahko bila raba ukrepa pridobivanja prometnih podatkov za nazaj dopustna morda zgolj za katalog kaznivih dejanj iz 2. odstavka 150. člena, in nikakor ne tudi 149.a člena ZKP (1. odst. 149.b člena).

IP glede 1. odst. 149.b člena ZKP ugotavlja, da je pridobivanje podatkov o prometu, kadar so potrebni za odkritje kaznivega dejanja in storilca, **zdaj izrecno omejeno na podatke »*v zvezi s komunikacijo osumljenca ali oškodovanca*«,** ter da je v 2. odst. izrecno določeno, da mora biti identifikacija komunikacijskega sredstva, za katerega se zahteva podatke, dovolj natančna, da zahtevek omejuje na vnaprej omejen in določljiv seznam oseb. S tem se nujno izključuje, da bi bilo mogoče na tej podlagi še mogoče pridobivati podatke o komunikacijskih sredstvih tretjih oseb, za katere v zahtevku ni ustrezno izkazano, da pripadajo osumljencu ali oškodovancu, ali podatke na nivoju »komunikacijskih sredstev«, kot so bazne postaje, omrežni usmerjevalniki in druga omrežna oprema, ki ni namenjena končnemu uporabniku. Obstoječi člen namreč na splošno govori o pridobivanju »*podatkov o prometu v elektronskem komunikacijskem omrežju*«, in ne zahteva tako določne opredelitve sredstva, kar, vsaj teoretično, omogoča tako pridobivanje podatkov o prometu o komunikaciji tretjih oseb kot tudi pridobivanje prometnih podatkov za omrežno opremo.

V skladu s predlaganim besedilom tega člena bo torej dovoljeno le pridobivanje podatkov o komunikaciji osumljenca ali oškodovanca, o komunikaciji tretjih oseb pa le, če so bili udeleženi v kateri od zajetih komunikacij osumljenca oz. oškodovanca.

Predlog predvideva tudi novo možnost pridobivanja podatkov (1. odst. v navezi z 2. in 4. odstavkom) v primeru, ko so podani razlogi za sum, da je bilo izvršeno, da se izvršuje oz. da se pripravlja oz. organizira kaznivo dejanje navedeno v katalogu, pa podatki niso potrebni za odkritje tega kaznivega dejanja oz. storilca, ampak »*zaradi preprečitve nastanka hujših posledic za življenje in zdravje*«. V teh primerih naj bi po vedenju IP šlo zlasti za pridobivanje podatkov za večje število oseb (t.j. izpiski prometnih podatkov za **vse telefone, priključene na bazne postaje na določenem območju**. Potreba po takšnih izpiskih naj bi se v preteklosti izkazala v nekaterih nujnih primerih (npr. pri iskanju storilcev kaznivega dejanja ugrabitve, kjer organi pregona ne razpolagajo z identifikacijo storilcev, ki pa po vsej verjetnosti za komunikacijo uporabljajo elektronske komunikacije; ali potencialno v primerih kraje orožja iz vojaškega skladišča; ali ponavljajočih se kraj železnine na širšem področju – vsi navedeni primeri so bili v preteklosti že uporabljeni kot primeri, kjer bi se zahtevalo večje količine prometnih podatkov, prav gotovo pa se bo v praksi poskušalo pooblastilo uporabiti še za marsikaj drugega). Pri tem sorodno pooblastilo za pridobivanje prometnih in lokacijskih podatkov v primerih varovanja življenja in telesa iz 153. člena ZEKom-1 ne bi zadostovalo[i].

IP takšni široki opredelitvi ni naklonjen, saj meji na zbiranje podatkov »na zalogo«, kar ni dopustno. IP prav tako meni, da v predlogu sprememb ni v zadostni meri predstavljena morebitna analiza tveganja predlaganega pooblastila za morebitne zlorabe pooblastila. Poleg tega pa iz obrazložitev ne izhaja utemeljitev njegove sorazmernosti glede na težo posegov v zasebnost posameznika, ki jo takšno pridobivanje osebnih podatkov predstavlja. Posledično pa tudi **predvidene varovalke niso zadostne**. Gre namreč za zahteve po podatkih o komunikacijah ne le za določeno komunikacijsko sredstvo temveč za vse komunikacije opravljene na področju pokrivanja ene ali celo več baznih postaj).

Kljub legitimnosti ciljev se je treba zavedati, da gre za neke vrste »**fishing ekspedicijo**« - pridobijo se podatki o vseh komunikacijah na določenem območju v določenem časovnem obdobju, potem pa se z analizo teh podatkov poskuša izluščiti, katere naprave so medsebojno komunicirale in njihove lokacije ter tako ugotoviti komunikacijske vzorce, ki bi lahko vodili v identifikacijo storilcev. Gre po naravi stvari za neciljan in široko usmerjen ukrep, saj se s tem pooblastilom zajema širok obseg podatkov nedoločenega

števila posameznikov, vključno s podatki o opravljenih komunikacijah v zaupnih razmerjih (komunikacija z odvetniki, zdravniki, verskimi osebami). Pridobitev vseh teh podatkov poleg potencialno koristnih podatkov za identifikacijo in izsleditev storilcev po naravi stvari pomeni poseg v temeljne človekove pravice širokega kroga oseb, ki nimajo absolutno nobene zveze s storilci preganjanega kaznivega dejanja in vodi v razkritje njihovih lokacij v času in prostoru, medsebojnih socialnih in komunikacijskih krogov, potencialno tudi razkritje osebnih podatkov občutljive narave (npr. oseb, ki so se nahajale v določeni zdravstveni ustanovi, pri verskem obredu, če je bilo zahtevano območje v bližini takšne ustanove).

Glede na navedeno menimo, da bi bilo takšno pooblastilo treba izločiti, če pa se predlagatelj vendarle odloči, da ga ohrani, bi bilo treba določiti, da se ga lahko uporabi zgolj **izjemoma in samo v najbolj nujnih primerih**, kar bi bilo treba jasno opredeliti, kot to npr. opredeljuje 4. alineja 1. odstavka 152. člena ZKP. Obravnavani člen v 4. odst. kot dodatno varovalko v tem primeru sicer predvideva, da morata tako operater oz. drug ponudnik storitev kot tudi policija v roku 8 dni od posredovanja o tem posredovanju obvestiti vse osebe, katerih podatki so bili tako pridobljeni[23].

Kljub obstoju te varovalke IP, kot smo izpostavili zgoraj, vseeno opozarja, da takšna različica ukrepa pomeni množični nadzor telekomunikacij. Zatorej je nujno, da so meje dopustnega pri njem jasno določene. IP predlaga, da se najprej podrobno in temeljito analizira dejanski obstoj potrebe po takšnem ukrepu in posledično ustrezno ugotovi, ali nujnost, primernost in sorazmernost predlaganega ukrepa resnično upravičujejo njegovo uzakonitev. V takšni analizi mora biti še posebej utemeljeno, v čem naj bi bile hujše posledice, ki naj bi jih z ukrepom preprečevali, in predvsem, kako naj bi jih posredovanje tako širokega nabora podatkov preprečilo. Če naj se predlagano vendarle uvede, morajo biti zagotovljene ustrezne varovalke pred zlorabo[24].

V kolikor se bo predlagatelj na podlagi navedenih dodatnih analiz vendarle odločil za uvedbo takšnega ukrepa, IP posledično predlaga, da bistveno dopolni določbo 2. odstavka o vsebini odredbe, tako da strožje opredeli pogoje za uvedbo takšnega ukrepa s ciljem preprečevati njegove morebitne zlorabe. Prav tako naj se čas, za katerega se pridobijo podatki, dodatno zameji na obdobje relevantnih dni in ur.

Kar zadeva vsebino odredbe (2. odst.), v tem primeru predlagamo, da se vanjo doda vse manjkajoče elemente odredb za zakonito prisluškovanje (1. odst. 152. člena) oz. preiskavo elektronskih naprav (3. odst 215. člena[25]), zlasti **utemeljitev oziroma ugotovitev neogibne potrebnosti** uporabe posameznega ukrepa v razmerju do zbiranja dokazov na drug način in uporabe ostalih milejših ukrepov, ter še opredelitev razlogov, iz katerih izhaja, da zadevni telekomunikacijski priključek dejansko uporabljata bodisi osumljenec bodisi oškodovanec.

Upoštevaje prakso z odredbami po ZEKom-1 pred zadevno odločbo Ustavnega sodišča (naslovniku se je vročalo zgolj »prepis tistega dela izreka odredbe pristojnega organa, v katerem je navedba vseh potrebnih podatkov o obsegu dostopa«, 1. odst. starega 166. člena), IP predlaga, da se v 2. odstavku 149.b člena določi, da se odredba naslovniku vroči v celoti (ne zgolj prepis prve strani). Na ta način lahko naslovnik pred pridobitvijo in posredovanjem podatkov preveri, ali so vsi pogoji za posredovanje podatkov izpolnjeni.

[23] To je lahko tudi s tehnično-izvedbenega vidika precej zahtevna obveznost, zlasti za policijo, zatorej predlagamo tudi, da, v kolikor navedena določba ostane v predlogu sprememb ZKP, njen tehnično-izvedbeni vidik v nadaljevanju predhodno uskladi vsaj s Sekcijo operaterjev pri GZS (SOEK) oz. MIZŠ. Treba je premisliti zlasti o določitvi kroga upravičencev do obveščanja (vsi, katerih kontaktni podatki so bili tako ali drugače pridobljeni) ter načinu obveščanja (npr. sms/klic/e-pošta/naslednji mesečni račun).
[24] Primerjaj nedavno sodbo v zadevi SZABO IN VISSY proti MADRŽARSKI, št. 37138/14, z dne 12. 1. 2016
[25] Glej tudi sodbo ustavnega sodišča v zadevi SIM kartica, ki je za prometne podatke, dobljene s preiskavo telefona, vzpostavila enako stopnjo varstva kot za prometne podatke, dobljene od operaterja.

Prav tako IP predlaga, da se na primernem mestu v ZKP **predvidi možnost, da se naslovnik odredbe pritoži zoper upravičenost odredbe, ne nujno zavoljo vsebinskih vzgibov[26] (ker ne bi želel dati podatkov) vsekakor pa, v kolikor meni, da** mu **takšna odredba nalaga nesorazmerno breme, ali če procesno ni popolna[27]**. Da ima lahko tretja oseba, pri kateri se opravljajo preiskovalna dejanja, pravni interes zahtevati pravno varstvo, potrjujeta nedavni odločbi Ustavnega sodišča št. U-I-193/15, Up-915/15[28]. V njih je sodišče potrdilo, da je država z izdajo odredbe za hišno preiskavo odvetniške pisarne, zoper katero potem pisarna (ki ni bila osumljenec) ni imela pritožbe, kršila njihove človekove pravice (vključno s pravico do komunikacijske zasebnosti iz 37. člena).

Utemeljitev tega sklepa sicer temelji na tem, da organom pregona ne sme biti na voljo neomejen dostop do (posebej zaščitene) spisovne dokumentacije odvetnika, vendar pa lahko po mnenju IP ista argumentacija, glede vsaj isto pomembne dobrine, velja tudi v zvezi s prometnimi podatki. Takšna pritožba bi omogočala preskus predvsem zgolj formalnih pogojev pravilnosti izdane odredbe (ne merituma), in bi torej lahko preprečila nekatere očitno pretirane odredbe, kot jih je zlasti zoper ponudnike spletnih storitev v preteklosti že videl IP (glej sklic na poročilo zgoraj). Pritožbo bi, glede na stanje stvari, lahko obravnavali bodisi zunajobravnavni senati, bodisi dežurni preiskovalni sodnik (a ne tisti, ki je odredbo izdal), bodisi določeni sodnik posameznik krajevno pristojnega okrožnega sodišča, kar se že ureja v 3. členu te novele. V primeru, da posebna pritožba ne bi bila omogočena, je – ob znatni širitvi možnih naslovnikov odredbe – za pričakovati, da bi lahko kateri od naslovnikov v posebej neutemeljenem primeru uporabil isto pravno sredstvo kot zadevne odvetniške pisarne, torej ustavno pritožbo.

Opcijsko bi bilo po mnenju IP nujno razmisliti o določitvi možnosti, da lahko naslovnik zahteva preizkus privzete 6-mesečne zakonske prepovedi razkritja odredbe (4. odst. 149.b člena ZKP). Predlog sicer predstavlja popravek obstoječega besedila, ker omogoča preiskovalnemu sodniku, da določi »drugačen« rok od privzetih 6 mesecev, torej teoretično tudi krajšega. Takšna možnost bi omogočila naslovniku, da v primerih očitno neutemeljenih odredb o tem še pravočasno obvesti posameznika, čigar podatke bi sicer moral posredovati, in bi slednjemu tudi omogočila, da se (kot subjekt postopka!) tudi sam zoperstavi odredbi.

Ker gre za pridobivanje podatkov za nazaj, po mnenju IP preprosto ni mogoče trditi, da bo vedno šlo za primere, ko bi razkritje dejstva, da se podatki pridobivajo, prohibitivno škodilo interesom preiskave. Alternativno predlagamo, da naj zakon po privzetem ne določa prepovedi razkrivanja, ampak naj to vedno določi preiskovalni sodnik, bodisi na podlagi lastne presoje, bodisi na podlagi utemeljenega predloga tožilca.

Kar zadeva možnost izdaje ustne odredbe v nujnih primerih (3. odst. 149.b člena), z naknadnim pisnim odpravkom, in že urejenim postopanjem v primeru, da se do priprave odpravka izkaže, da odredba ni bila utemeljena, IP meni, da v primeru, ko je bil pisni odpravek potem poslan, ali pa je bilo posredovanje preklicano, preden se je zgodilo, ni potrebe po obveščanju prizadetih uporabnikov (4. odst.).

Končno velja kot dodaten argument za izključitev oziroma bistveno zamejitev predlaganega ukrepa v predlogu sprememb ZKP opozoriti, da se s formalno širitvijo ukrepa tudi na 'neoperaterje' veča možnost, da preiskovalci pri tem **pridobijo tudi podatke, s katerimi naslovnik v času prejema zahtevka ne bi več smel razpolagati.** Zelo verjetno namreč v praksi marsikdaj, kateri izmed upravljavcev spletnih strani hranijo prometne podatke o svojih uporabnikih, brez da bi za to zagotovili jasno pravno podlago, oz. jih hranijo bistveno dlje, kot bi jih, upoštevaje načelo sorazmernosti iz 3. člena ZVOP-1, smeli. Takšna hramba pri njih

[26] Primerjaj z medijsko nedavno zelo odmevno ameriško zadevo z sodno odredbo podjetju Apple, da s pripravo posebne posodobitve mobilnega operacijskega sistema iOS omogoči pridobitev prometnih podatkov in drugih forenzičnih podatkov z zaklenjenega in šifriranega mobilnega telefona storilca terorističnega napada; podjetje Apple je sicer zahtevek zavračalo iz vsebinskih razlogov.
[27] Kar ustreza ameriškemo kazenskoprocesnemu instrument predloga za razveljavitev odredbe (motion to quash)
[28] http://odlocitve.us-rs.si/sl/odlocitev/US30878

pa, za razliko od operaterjev, pravno ni v zadostni meri zadovoljivo regulirana. Poleg tega je nemogoče zagotoviti vnaprejšnji zunanji nadzor vseh podatkov, ki jih hranijo vsi operaterji. Na temeljno zakonitost obstoja hranjenih podatkov bosta zato, morala v tem primeru paziti tudi policija in državni tožilec in postopati previdno, in npr. v primeru, da prejmeta tudi prometne podatke, stare po več let, ustrezno vnaprej preveriti, ali jih je naslovnik še zakonito hranil.

Pridobivanje prometnih podatkov za naprej – data freeze (nov 149.c člen ZKP)

Nov 149.c člen ZKP omogoča, da policija zaprosi operaterja oz. drugega ponudnika storitve, da začne za določenega uporabnika ločeno shranjevati podatke o prometu (t.i. *data freeze*), za obdobje največ 3 mesecev, ter da mu jih potem posreduje na naknadno zahtevo. Ta naknadna zahteva lahko pride najprej 8 dni po zajemu podatkov, razen če gre za katero od hujših kaznivih dejanj, ali če gre za sledenje ukradenega telefona. V teh primerih se podatke lahko začne pridobivati takoj, oz. sproti.

Navedeni ukrep ne zahteva vnaprejšnje in neselektivne retencije, ampak le hrambo podatkov od osumljenca, oz. nezakonitega uporabnika sredstva (v primeru tatvine). Posledično je ukrep mogoče uporabiti tudi za lažja kazniva dejanja (zagroženo vsaj 1 leto zapora). Z odlogom pridobitve podatkov, razen kot zgoraj, pa se prepreči uporabo ukrepa za sledenje osumljenca v realnem času. V primeru, da se sledi ukradenemu telefonu, je dodana obveza, da se uporabnika telefona v 8 dneh po izvedbi odredbe obvesti, da se mu je sledilo.

IP pričakuje, da se bo posledično ustrezno zmanjšalo število odredb za ukrep po 149.b členu.

Člen 149 c se v veliki meri sklicuje na prejšnjega, zato IP v izogib ponavljanju opozarja, da veljajo iste pripombe, kot so glede vsebine odredbe, določnosti opredelitve komunikacijskega sredstva, možnosti ugovora in obveznosti razkritja podane v zvezi s predhodnim členom.

Glede 6. odstavka predlaganega 149.c člena IP meni, da bi bile v tem delu potrebne dopolnitve, s katerimi bi zagotovili njegovo nedvoumno in ozko tolmačenje z vidika dopustnega ozkega obsega posega v komunikacijsko zasebnost. Naveden člen namreč nikakor ne bi smel biti podlaga za zahteve oziroma pridobivanje podatkov, ki se nanašajo na vsebino komunikacije, niti ne bi smelo biti na njegovi podlagi dopustno odrediti *hrambe vsebine komunikacije.* V praksi pa bi po mnenju IP upoštevajoč trenutno besedilo lahko prihajalo do različnih implementacij predlaganega 1. odstavka 149.c člena.

Pridobivanje podatkov o lastniku komunikacijskega sredstva, oz. o obstoju njegovega pogodbenega razmerja (nov 149.č člen ZKP)

Zadevni člen na novo ureja 3. odst. 149.b člena, s čimer policiji omogoča, da na svojo zahtevo (torej brez odredbe) od operaterja oz. ponudnika storitve pridobi podatke o lastniku oz. uporabniku določenega komunikacijskega sredstva. Člen je zavoljo nekaterih negativnih izkušenj iz prakse (pridobivanje podatkov o prometu na ta način) dopolnjen tako, da izrecno prepoveduje pridobivanje podatkov o prometu oz. podatkov o vsebini komunikacije (vključno s podatki o času, ko je bilo sredstvo v rabi, kar je bilo do sedaj dovoljeno), ter tako, da daje naslovniku možnost, da v primeru ocene, da zahtevek ni zakonit, podatke namesto policiji posreduje krajevno pristojnemu sodišču v preverbo. Prepoved obveščanja uporabnika velja tri mesece, se pa, v kolikor v tem času prispe še sodna odredba po 149.b ali 149.c členu, ustrezno podaljša.

Možnost vročitve odgovora sodišču po mnenju IP vsebinsko pravzaprav že predstavlja pritožbo zoper zahtevek policije. IP ga kot takega podpira, vseeno pa predlaga, da se, kot je navedeno zgoraj v zvezi s predhodnimi členi, predvidi celovitejša možnost pritožbe na zunajobravnavni senat oz. sodnika posameznika.

Pridobivanje naročniških podatkov s strani zasebnega tožilca (nov 149.d člen ZKP)

Določba 1. odstavka predlaganega 149.d člena, da oseba lahko ob vložitvi zasebne tožbe od sodišča zahteva, da na podlagi razpoložljivih identifikacijskih podatkov o določljivem storilcu kaznivega dejanja »pridobi njegove osebne podatke iz zbirk osebnih podatkov«, je zelo široka, saj ni omejena ne glede nabora osebnih podatkov, ki jih mogoče pridobiti, ne glede upravljavcev, od katerih bi bilo mogoče te podatke pridobiti. Menimo, da bi bilo tako z vidika zagotavljanja doslednega izvajanja načela sorazmernosti kot tudi določljivosti obdelavo osebnih podatkov in posledično pravne varnosti treba določiti omejitev glede dopustnega obsega pridobivanja podatkov v smislu pridobitve le tistih osebnih podatkov, ki so potrebni za enolično identifikacijo storilca, saj je – kolikor razumemo – ravno to povod za predlagane določbe (t.j. primeri ko zasebni tožnik razpolaga le z vsebino sporne objave, ne razpolaga pa z drugimi identifikacijskim podatki, da bi lahko vložil tožbo zoper *znanega* storilca).

Menimo, da člen, kot je spisan, dejansko sploh ne doseže zasledovanega cilja. Srž problematike je namreč v tem, da oseba, ki je npr. bila razžaljena zaradi določene objave na spletu, nima podatkov o identiteti pisca, za vložitev zasebne tožbe proti njemu. Predlagani člen naj bi s posredovanjem sodišča to omogočil, obenem pa določba 3. odstavka prepoveduje pridobivanje podatkov o komunikacijah, torej tudi prometnih podatkov. V praksi torej zasebni tožnik ne bo mogel pridobiti IP naslova pisca, bo pa dobil morebitne podatke o elektronski pošti in druge podatke, ki jih je moral pisec ob registraciji zaupati spletnemu ponudniku (slednji so pogosto izmišljeni, saj praviloma pisci vsebin, ki bi lahko bile predmet tožb ali pregona kaznivih dejanj, ne navajajo svojih pravih podatkov ob registraciji).

IP pa ocenjuje kot primerno določbo, da se lahko zahtevek poda šele ob vložitvi zasebne tožbe (zato, da se prepreči špekulativno pridobivanje podatkov). Prav tako pa predlaga, da se v dani člen doda možnost odgovora preiskovalnemu sodniku, oz. polno možnost pritožbe, kot zgoraj.

K. 33. členu predloga ZKP-N (nov 150.a člen ZKP, IMSI lovilci)

Kot izhaja iz uvodne obrazložitve, se »*z vidika povečevanja učinkovitosti dela organov pregona in preiskovanja kaznivih dejanj uvaja možnost uporabe t.i. IMSI lovilca*«. Lovilec je naveden kot »*posebna tehnična sredstva*«, z njim pa se sme ugotavljati 1) »***podatke za razpoznavo** številke komunikacijskega sredstva in številke za elektronsko komuniciranje*«, oboje za namen priprave [ukrepov pridobivanja prometnih podatkov na nazaj/naprej po novih 149.b in 149.c členih, oz. za izvedbo prisluškovanja po 1. tč. 1. odst. obstoječega 150. člena], ter 2) **(podrobnejšo) »*lokacijo komunikacijskega sredstva*«**. Predlog v veliki meri že upošteva pripombe IP k predlogu prejšnje novele ZKP[29], zato dodajamo le tiste pripombe, za katere menimo, da so še dodatno potrebne, obenem pa v ilustracijo narave posega, ki ga predstavlja lovilec, dodajamo še opis njegovega delovanja.

Uvodno o delovanju IMSI lovilca

IMSI lovilec, angleško *IMSI catcher*, *Stingray*[ii] oz. *Cell site simulator (CSS)*, je naprava za diagnosticiranje in nadzor uporabnikov mobilnih telefonskih omrežij. Gre za mobilno oddajno-sprejemno napravo različnih oblik (ročna, prenosna, za v vozilo), ki je sposobna simulirati bazno postajo mobilne telefonije (angl. *cell site*). Na ta način lahko nase pritegne bližnje mobilne telefone, jih s tem začasno ali trajno odklopi od pravega omrežja, od njih pridobi določene podatke (zlasti IMSI in IMEI številki), v naprednejših različicah pa jih tudi

[29] https://www.ip-rs.si/fileadmin/user_upload/Pdf/pripombe/MP.pdf__novela_ZKP-M.pdf__dec_2013.pdf

onemogoči, jim izprazni baterijo, prisluškuje, ali celo opravlja omrežne storitve v njihovem imenu. Uporabnik mobilnega telefona ves ta čas meni, da je še vedno priklopljen na svojega mobilnega operaterja, čeravno bi lahko ob skrbni rabi opazil, da mu vse storitve ne delujejo. Bolj napredne različice lovilcev omogočajo tudi sprotno pridobivanje prometnih podatkov oz. prisluškovanje telefonu (zanimivo za zasebne uporabnike), nameščanje zlovešče programske opreme na telefone za potrebe nadaljnjega nadzora (zanimivo tako za zasebne kot vladne uporabnike), oz. takojšnjo izvedbo ukrepov prisluškovanja in pridobivanja prometnih podatkov skozi neposredno povezavo z operaterji.

Lovilec za svoje delovanje izkorišča nekatere strukturne pomanjkljivosti 2G (GSM) mobilnega omrežja[30], predvsem dejstvo, **da bazni postaja telefonu ni treba dokazati, da je pristna.** To praktično pomeni, da lahko neka tretja oseba (policija, varnostno-obveščevalna služba, ali celo zasebna entiteta) postavi novo bazno postajo, ter jo nastavi tako, da se predstavlja kot npr. Telekomova bazna postaja, s čimer doseže, da jo bodo bližnji telefoni prepoznali kot Telekomovo bazno postajo, in ji tudi zaupali kot takšni.

Za razumevanje dejanj, ki lovilcu omogočajo delovanje, je potreben vsaj osnovni opis delovanja GSM omrežja. Mobilni telefon ob vklopu (*power on* ali povrnitev nazaj iz načina brez povezave) opravi sken prisotnih baznih postaj, ter se potem skuša povezati na najmočnejšo bazno postajo njegovega operaterja, oz. (zlasti v tujini) operaterja, ki mu omogoča gostovanje. Proces povezave se imenuje *IMSI attach*, in v njem telefon mobilnemu omrežju pošlje svojo naročniško številko (t. i. IMSI številka, kar je uporabnikova naročniška številka in ne telefonska številka), obenem pa z rabo šifrirnega ključa, ki je shranjen na vanj vstavljeni SIM kartici, omrežju dokaže, da je to resnično njegova številka. V zameno dobi t. i. »začasno naročniško številko« (TMSI), preko katere se operaterju izkazuje v vseh sledečih komunikacijah, omrežje pa ga zabeleži kot prisotnega v omrežju na določenem segmentu omrežja (npr. v Lokacijskem območju št. 1, Ljubljana). Po tem telefon preide v neaktivni način (*idle mode*) in prekine povezavo z omrežjem. Temu se ne javlja tudi ob manjših premikih, ko zazna, da je bližje kakšni drugi bazni postaji, dokler ta pripada istemu lokacijskemu območju (skratka, ob premiku iz centra mesta v drugo četrt se mu ni treba posebej javiti). Posledično telefonu ni treba voditi stalne povezave z omrežjem, saj bi to zahtevalo znatno porabo baterije. Vendar pa se bo vedno in takoj javil omrežju, če bo zaznal, da se je premaknil tako daleč od izvorne bazne postaje, da je že prešel v novo Lokacijsko območje, npr. št. 2, Grosuplje (*random location update, RLU*). Prav tako bo omrežju občasno, za vsak primer, javil, v katerem območju se nahaja (*periodic location update, PLU*). Tako omrežje približno ve kje je, za primer, če bi moralo omrežje telefonu dostaviti kakšno storitev (klic, sms, podatke). Ko se to zgodi, omrežje telefonu pošlje *paging request* za natančno lokacijo (na nivoju bazne postaje) in za čas trajanja prenosa prevzame nadzor nad telefonom. Po koncu npr. klica pa telefon spet postane *idle*, in se javlja zgolj periodično oz. po večjih geografskih premikih.

Če ponazorimo z (namišljenim) primerom. Policija lovilca aktivira na primerni lokaciji ob Trgu republike v Ljubljani, kjer v danem trenutku poteka državna proslava in kjer je zato v določenem trenutku prisotnih več kot 1000 povabljenih gostov in drugih obiskovalcev, (skoraj) vsi s telefonom v žepu. Dobra polovica, recimo 600 telefonov, uporablja Telekomovo omrežje. Ti telefoni trenutno zaznavajo prisotnost več baznih postaj, npr. A038 (Cankarjev dom) in A075 (Vlada RS), A109 (Nama), in A074 (Kongresni trg). Večina jih kot najmočnejšo bazno postajo vidi to na Cankarjevem domu (A038), drugi pa zavoljo njene prezasedenosti uporabljajo druge postaje. Prek njih komunicirajo z omrežjem, ko pošiljajo SMS-e, oz. ko brskajo po spletu in objavljajo fotografije iz dogodka. Na tej točki policija prižge svojega lovilca in ga nastavi, da se predstavlja kot Telekomova bazna postaja (prvi policijski ukrep). Vsi telefoni jo v nekaj sekundah prepoznajo kot najmočnejšo bazno postajo. Vsi ti telefoni se bodo torej od tega trenutka naprej za potrebe storitev omrežja, skušali obrniti nanjo. Vendar, ker gre za postajo v istem lokacijskem območju (Ljubljana), ji sicer sami ne pošljejo ničesar, razen ko poteče rok za naslednje periodično javljanje (takrat ji sporočijo: »telefon s TMSI še

[30] Pri 3G oz. 4G telefonih dejstvo, da zavoljo kompatibilnosti s starejšimi omrežji še vedno omogočajo nekatere od opisanih napadov, oz. je telefone z motenjem 3G/4G signala mogoče spraviti nazaj na 2G.

vedno tukaj«). Policija ne želi čakati na vsa ta javljanja, pa tudi sicer si s TMSI-jem težko kaj pomaga, ker je začasen. Zato lovilca nastavi tako, da se telefonom predstavi kot bazna postaja v lokacijskem območju npr. Grosuplja. To je drug policijski ukrep. Telefoni to zaznajo, in ker je to tudi najmočnejša postaja, telefoni to prepoznajo kot znak, da se je njihov lastnik vmes premaknil v Grosuplje. Nemudoma se javijo bazni postaji s sporočilom omrežju, da so zdaj v Grosuplju (Random Location Update, »sporoči omrežju, da se je telefon s TMSI 123 prestavil v Grosuplje«). Lovilec sprejme ta zahtevek, nato pa telefonu sporoči (tretji policijski ukrep), da je z njegovo sejo nekaj narobe in da se naj poveže na sveže (zahteva nov *IMSI Attach*, »prišlo je do napake v seji, prosimo, prijavite se znova«). Telefon stori, kot naročeno, pri čemer tokrat pošlje svojo pravo IMSI številko (»telefon z IMSI xxxxxxxxx tukaj, javljam se v vaše omrežje«). Na podoben zahtevek pošlje še številko naprave (IMEI številko). Lovilec tako v času nekaj deset sekund do nekaj minut razpolaga z IMSI in IMEI številkami vseh prisotnih Telekomovih telefonov. Ta postopek je z lovilcem mogoče ponoviti tudi za vse druge operaterje, ter s tem pridobiti polni seznam udeležencev na določenem območju oz. v njegovi neposredni bližini.

Naj na tem mestu dodamo, da lovilec na ta način ne more dobiti tudi telefonske številke (MSISDN). Ta se tekom prijave v omrežje ne posreduje, saj za to ni prave potrebe. Da bi dobila to, bi morala policija bodisi vprašati operaterja, uporabiti medoperaterski (SS7) dostop, ali aktivno prisluškovati, dokler se med telefonom in omrežjem ne zgodi kakšna operacija (npr. poslan SMS), ki nosi to informacijo. Ampak za potrebe sprožitve ukrepa po 1. al. 1. odst. 150. člena ZKP policiji zadostuje že podatek o IMSI številki.

Vprašanje je seveda, kako policija izve, katera IMSI številka pripada določeni osebi. Če je na osamljenem geografskem območju, tega ni težko ponoviti, sicer pa mora policija z lovilcem slediti osumljencu in meritev ponoviti na več lokacijah. Vsakič bo zajela nekaj 10 do nekaj 100 IMSI številk. Tista, ki bo prisotna v vseh zajemih (*cross-match*), bo osumljenčeva. Včasih to sicer ni bistveno. Za popis npr. prisotnih na predstavi mora policija zgolj poslati operaterju seznam IMSI številk, in po obstoječem 3. odst. 149.b člena ZKP lahko (brez odredbe!) prejme imena naročnikov, oz. podatek, da gre za predplačnike.

Po prejemu IMSI številke lovilec preprosto zavrne telefon (*Attach fail*), ter mu s tem naroči, naj se vrne h kateri od ostalih baznih postaj. Telefon to tudi izvede. Vse skupaj lahko traja le nekaj sekund, večina mobilnih telefonov pa uporabniku nikoli ne sporoči, da je karkoli šlo narobe.

Opisano (pridobitev IMSI številk vseh telefonov na določeni lokaciji, oz. določitev IMSI številke določenega uporabnika) je le najosnovnejša zmogljivost lovilca. Nadaljnjih uporab je več, od določitve natančne lokacije določenega telefona, pa vse do prisluškovanja telefonu. Njihov nabor je odvisen od tehničnih zmogljivosti lovilca, značilnosti prisotnih omrežij, ter motivacije uporabnika lovilca.

Za policijo je najbolj zanimiva določitev mikro lokacije osumljenca, za katerega policija že pozna IMSI (oz. telefonsko) številko. Scenarijev za to je več, tipično pa zadevajo lociranje osumljenca (ali žrtve kaznivega dejanja) bodisi v gosto poseljenem urbanem okolju (blokovska naselja). Policija začne s tem, da se obrne na operaterja in ga zaprosi za lokacijske podatke z določeno številko. Na podlagi njih, npr. ugotovi, da se osumljenec zvečer vedno zadržuje v določenem blokovskem naselju. Odpravi se tja, vklopi lovilec, nastavi ga kot bazno postajo osumljenčevega omrežja, ter ponovi zgoraj opisan postopek. Vendar po izvedenem *Attach* postopku telefona ne pošlje stran. Namesto tega ga postavi v aktivni način (da bi izvedla storitev), in mu naroči, naj okrepi svoj signal, da ta na lokaciji lovilca zrase z recimo -100dBm na -70dBm (30dBM, 1000x močnejši signal). Nato začne premikati lovilec v različne smeri in spremljati, kaj se zgodi z jakostjo signala. Bolj rase, bližje iskanemu telefonu je lovilec. Na ta način lahko policija določi, v katerem bloku se nahaja iskani. Za določitev konkretnega stanovanja po navadi uporabi drugo, bolj prenosno in manj aktivno opremo, s katero lažje hodi od vrat do vrat in vsakič izmeri seznam[iii].

Naslednji uporabi lovilca sta izpraznjenje uporabnikove baterije oz. onemogočenje povezovanja v matično omrežje. Kot že rečeno, lahko lovilec telefonu naroči, da naj okrepi signal, kar bo, slej ko prej, izpraznilo njegovo baterijo. Dalje mu lahko sporoči lažne podatke o njegovem omrežju, tako da se telefon več ne bo hotel povezati nazaj na druge bazne postaje. Slednje se lahko razreši zgolj s ponovnim zagonom telefona.

Možno pa je tudi prisluškovanje sms-om in klicem (zlasti odhodnim). Lovilec lahko po tem, ko prevzame nadzor nad določenim telefonom, dejansko vzpostavi povezavo z omrežjem[iv]. Po tem se nahaja na sredini med telefonom in omrežjem in lahko izvaja t.i. *man–in-the-middle* napad. Ko uporabnik pošlje sms, ga lovilec sprejme, kopijo pa pošlje naprej v omrežje, v imenu dejanskega pošiljatelja. Podobno lahko izvede tudi klice, in, z najnovejšo opremo, velja enako tudi za podatke. Vsebina prejetih sms-ov idr. je sicer načeloma šifrirana, vendar lahko imetnik lovilca šifriranje bodisi izklopi, ali vklopi zgolj šibko šifriranje, ki ga lahko sproti razbije. Najbolj motiviran uporabnik (varnostno-obveščevalne službe, zasebne varnostne agencije) se lahko omrežju tudi predstavijo kot pravi uporabnik. Za to rabijo kopijo uporabnikove SIM kartice (na kateri so šifrirni ključi), ki jo lahko dobijo s kloniranjem, od operaterja, ali od proizvajalca SIM kartic. Če se uspejo premikati skupaj z uporabnikom, mu lahko na ta način (sicer z znatnimi stroški) prisluškujejo povsem brez posredovanja operaterja. Prav tako se lahko omrežju predstavijo kot on, in vršijo klice pod njegovo identiteto.

Policija lovilcev praviloma ne uporablja za prisluškovanje, ker lahko to izvede kar preko operaterja[v].

a) glede rabe IMSI lovilca za potrebe identificiranja osumljenčevega mobilnega telefona (IMEI številke) oz. naročniških podatkov (IMSI številka, MSISDN oz. telefonska številka):

Glede opredelitve tehničnega sredstva:

Čeprav iz obrazložitve predloga (tako uvodne, kot k temu členu) na več mestih jasno izhaja, da predlagani prikriti preiskovalni ukrep (PPU) zajema zgolj rabo specifičnega tehničnega sredstva, 33. člen pokriva zgolj rabo prikritega preiskovalnega ukrepa uporabe posebnega tehničnega sredstva za nadzor rabe mobilnih telefonov in drugih naprav, ki uporabljajo mobilno omrežje ponudnika mobilne telefonije (torej IMSI lovilca). To v uvodnem odstavku ni ustrezno zapisano. Ukrep je namreč zelo splošno poimenovan kot »*posebna tehnična sredstva*«, ki omogočajo ugotavljanje določenih podatkov, med njimi razpoznavo »*številke komunikacijskega sredstva*«, »*številk za elektronsko komuniciranje*«, oz. »*lokacije komunikacijskega sredstva*«. Izbira tako splošnega izrazoslovja najbrž sledi želji, biti ustrezno tehnološko nevtralen, vendar je v danem primeru **tako ohlapna, da, vsaj teoretično, dopušča tudi rabo povsem tretjih naprav, ki nimajo nič z IMSI lovilci**.

Po mnenju IP bi namreč v ta opis lahko sodil tudi nadzor drugih komunikacijskih sredstev, npr. interneta. IP je npr. seznanjen s poskusi identifikacije kolovodij napadov porazdeljene ohromitve storitve (DDOS napadi), ki so jih februarja 2012 domnevno vršili člani slovenskega Anonymousa[vi], oz. napori nekaterih tujih policij, ki so po pridobitvi nadzora nad določenimi nezakonitimi spletnimi stranmi poskušali identificirati uporabnike (t.j. pridobiti njihove IP številke), tako da so v kodo spletne strani vstavili zloveščo kodo, ki jih je obvestila o uporabnikovi pravi identiteti. V obeh primerih je šlo za identifikacijo uporabnikov TOR anonimizacijskega omrežja. Odstavek, kot je napisan, bi bilo mogoče razumeti kot dovoljenje tudi takšnih aktivnosti, ki seveda odpirajo kompleksna vprašanja posegov v uporabnikovo zasebnost.

IP posledično predlaga, da se odstavek v skladu z načelom zakonitosti precizira, tako da bo jasno, da gre za napravo za nadzor signala mobilne telefonije, ali za »simulator bazne postaje mobilne telefonije«, kar tipično opiše vse značilnosti naprave.

Glede vsebine odredbe:

IP predlaga, da se v člen vrine nov četrti odstavek, ki bi točneje opredelil vsebino zahtevane sodne odredbe za uporabo lovilca. V njej bi morale biti po mnenju IP smiselno vključene vse sestavine, ki jih določa 1. odst. 152. člena ZKP (odredba za zakonito prisluškovanje), torej:

- cilj uporabe (1. ali 2. tč. 1. odst),
- kateri lovilec se bo uporabil, ter kakšne so njegove natančne tehnične zmogljivosti (strojne in programske);
- podatke o osebi, katere številko je potrebno pridobiti, oz. ki jo je treba locirati;
- utemeljitev razlogov za sum, da se izvaja kaznivo dejanje, ter razlogov za sum, da zadevna oseba uporablja mobilno komunikacijsko sredstvo;
- utemeljitev nujnosti rabe ukrepa (nesorazmerne težave z ostalimi ukrepi).

Glede načina izvedbe:

IP podpira zamisel, da naj se lovilci hranijo na sedežih okrožnih sodišč (6. odst. 150.a člena ZKP), ter da naj se prevzemajo na podlagi predložitve odredbe za njihovo uporabo in vrnejo takoj po sestavi zapisnika. IP zavoljo dosledne izvršitve 7. odstavka 150.a člena ZKP, torej prepovedi uporabe lovilca za druge namene (prisluškovanje, kot opisano zgoraj), oz. prepovedi uporabe lovilcev, ki to omogočajo, predlaga, **da policijo med rabo lovilca ves čas spremlja tudi preiskovalni sodnik, in spremlja rabo lovilca.**

IP z namenom boljšega nadzora in transparentnosti uporabe tovrstnih ukrepov predlaga tudi, da se v zapisnik o izvedbi ukrepa (4. odst. 150.a člena ZKP) vključi tudi podatek o proizvajalcu in modelu lovilca, ter verziji programske opreme, ki teče na njem.

IP se strinja, da je nujna predvidena določba, da se številke zajetih tretjih oseb nemudoma uniči.

Glede naprednejših rab lovilca:

Kot že omenjeno, 7. odstavek 150.a člena ZKP predvideva, da se ne smejo uporabljati takšni lovilci, ki omogočajo ali bi lahko omogočali prisluškovanje in snemanje elektronskih komunikacij.

IP v zvezi s tem opozarja, da glede na javno dostopne informacije (pridobljene in objavljene na podlagi zahteve za dostop do informacij javnega značaja s strani tretjega posameznika[31]), vsaj eden od dveh oz. treh lovilcev, s katerimi naj bi razpolagala policija (Syborg oz. zdaj Verint GI2 interogator) omogoča tudi takšne aktivnosti[32]. Le te so na voljo kot dodatni programski moduli oz. nadgradnje. IP prav zato, s ciljem preprečitve takšne rabe, opozarja na nujnost dopolnitve navedenih določb z zahtevo, da bi vsako rabo lovilca spremljal tudi preiskovalni sodnik.

b) glede rabe IMSI lovilca za potrebe lociranja osumljenca, oz. drugih iskanih oseb:

Kot že utemeljeno zgoraj pri členih o prometnih podatkih, predstavlja IMSI lovilec hujši poseg v zasebnost od rabe klasičnih tehničnih naprav za lociranje osumljenca (t.j. npr. GPS oddajnika). IP zatorej, v kolikor se bo predlagatelj zakona odločil za uzakonitev rabe lovilcev, opozarja, da mora biti ta strogo omejena na ozko določene primere preiskave zgolj najhujših vnaprej določenih kaznivih dejanj, torej na iskanje obdolženca zgolj v povezavi s preiskavo kaznivih dejanj iz kataloga po 150. členu ZKP.

[31] https://slo-tech.com/forum/t631145/0

[32] Glej javno dosegljivo dokumentacijo izdelka, http://fundacja.lexnostra.pl/wp-content/uploads/2012/08/Engage_Gi2_User_Manual_v38.pdf, poglavje 3, opcijske komponente

Kot zgoraj pojasnjeno v delu o delovanju lovilcev, mora lovilec za lociranje mobilnega telefona oz. drugačne mobilne naprave le-to vezati nase, ter jo tudi aktivno nadzorovati. Posledično takšna raba vedno presega elemente pasivnega prisluškovanja, zatorej IP tudi v tem primeru predlaga, da naj policijo tekom rabe spremlja preiskovalni sodnik.

K 35. členu predloga ZKP-N (preciziranje obveznosti policije glede ravnanja s posnetki, pridobljenimi z ukrepi po 149.a, 149.b in 149.c, ter 150., 150.a in 150.b členih ZKP)

IP vsekakor podpira **razširitev** obveznosti policije, da po zaključku uporabe prikritih preiskovalnih ukrepov vse z njimi pridobljeno gradivo, skupaj s poročilom, preda državnemu tožilcu, ki ga potem (v kopiji) preda še preiskovalnemu sodniku v preizkus, **tudi na pridobljene podatke o prometu** (149.b/149.c člena ZKP) oz. na podatke, pridobljene z IMSI lovilcem.

IP bi glede na nekatere nejasnosti, ki jih je zaznal tekom svojih inšpekcijskih postopkov, predlagal dodatno dopolnitev, in sicer, da se besedilo prvega odstavka še bolj precizira tako, da ne bo nobenega dvoma o tem, da mora policija predati posnetke idr. **v vseh izvodih, vključno z morebitnimi kopijami, oz. da mora po predaji gradiva morebitne svoje lastne kopije, izbrisati oz. drugače uničiti, ne glede na morebitne drugačne določbe zakona, ki ureja hrambo arhivskega gradiva**.

Navedeno konkretno izvira iz skrbi IP, da bi v praksi sicer policija tudi po podaji kazenske ovadbe lahko štela za zakonito hrambo npr. DVD nosilcev z rezultati telefonskega prisluškovanja kot arhivskega gradiva (npr. kot kopijo podane ovadbe tožilcu). Takšen režim, kjer policija po zaključku preiskave ne hrani več niti kopije gradiva, ki predstavlja očiten (a začasno dovoljen) poseg v komunikacijsko zasebnost osumljenca, ter drugih oseb, katerih podatki so bili zajeti v komunikaciji z njim, je glede na ustavni položaj komunikacijske zasebnosti po mnenju IP edini primeren. Po mnenju IP takšen režim sicer izhaja tudi iz (prav tako spremenjenega) sledečega člena, ki določa režim hrambe gradiva pri državnem tožilcu, in glede tega določa, da se mora gradivo v primeru odstopa od ali zastaranja pregona zapisniško uničiti, ter še posebej, da se mora določeno privilegirano gradivo (novi 222.a člen ZKP) po potrebi takoj zapisniško uničiti.

K 36. členu predloga (sprememba 154. člena, hramba izsledkov prikritih preiskovalnih ukrepov na sodišču)

IP podpira novo predlagano možnost takojšnje izločitve privilegiranih podatkov (komunikacija osumljenec – odvetnik ipd., kot to določa novi 222.a člen) iz rezultatov gradiva prikritih preiskovalnih ukrepov po 150. in 151. členu (prisluhi) oz. 155.a členu ZKP (tajno delovanje), ki naj jo odredi za to določen sodnik (ne preiskovalni sodnik) tekom posebnega *ex parte* naroka.

IP predlaga, da se ta možnost predpiše tudi za podatke, pridobljene z ukrepi po 149.b in 149.c členih ZKP.

K 37. členu (sprememba 156. člena, pridobivanje bančnih podatkov osumljenca)

IP podpira dodatno kvalifikacijo v 5. odstavku, ki zdaj jasneje pojasnjuje, da policija oz. državni tožilec od banke na podlagi svoje zahteve (torej brez sodne odredbe) ne moreta pridobiti podatkov o »*premoženjskem stanju osumljenca oz. stanju vlog in depozitov ter o stanju in prometu na računih*«, temveč le podatke o tem, kdo je lastnik določenega računa, kdaj je bil ta račun v uporabi, oz. ali banka posluje z določenim osumljencem.

V upanju, da boste predstavljene obsežne pripombe na predlagano besedilo sprememb ZKP upoštevali v nadaljnji pripravi sprememb zakona, vas lepo pozdravljamo.

S spoštovanjem,

Mojca Prelesnik, univ.dipl.prav.,
informacijska pooblaščenka

[i] Tu se namreč sme pridobit podatke le za osebo, katere življenje je v nevarnosti, ne ap tudi podatkov drugih oseb.
[ii] »Stingray« je pogovorno ime za takšno napravo v ZDA, kjer gre za široko uporabljani izdelek proizvajalca Harris Communications.
[iii] Na ta način je ameriški FBI v preteklosti uspešno lociral Daniela Ringmaidna, osumljenega več davčnih utaj, za katerega dotlej niso vedeli, kdo je, vedeli pa so le, da svoja kazniva dejanja izvršuje preko prenosnega računalnika, ki je v internet priključen preko Verizonovega 3G vmesnika (ang. *dongle)* (se pravi, preko mobilnega telefona). Ker za to dejanje niso imeli odredbe, se je Ringmaiden kasneje uspešno izpogajal za zaporno kazen v dolžini prestanega pripora, in bil po tem tudi izpuščen na prostost.
[iv] Praviloma s svojo SIM kartico.
[v] Pravzaprav imajo novejše različice Harrisovih lovilcev, ki jih že imajo nekatere ameriške pravosodne službe, poleg lovilca integriran CALEA vmesnik, ki jim omogoča, da takoj po ugotovitvi IMSI številke preko ustne odredbe preiskovalnega sodnika naročijo prisluškovanje in prometne podatke, pri čemer te prejmejo neposredno v vmesnik v prisluškovalnem kombiju. Takšne operacije izvajajo zlasti zavoljo nacionalne varnosti (varovanje predsednika na javnih dogodkih), oz. zoper kriminalne družbe, osumljene proizvodnje in trgovine z drogami (DEA).
[vi] https://www.cert.si/si-cert-2012-03-napadi-na-slovenske-spletne-strani/